

Autodefensa Digital

Contraseñas seguras,
archivos cifrados



Contraseñas seguras

<p>□□□□□□□□□□□□□□□□</p> <p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor &3</p> <p>CAPS? □</p> <p>COMMON SUBSTITUTIONS □□□</p> <p>NUMERAL □□□</p> <p>PUNCTUATION □□□□</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)</p>	<p>~28 BITS OF ENTROPY</p> <p>□□□□□□□□ □□□□□□□□ □□□□ □□□□</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>□□□□□□ □□□□□□ □□□□□□ □□□□□□ □□□□□□ □□□□□□ □□□□□□ □□□□□□</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>□□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED
EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS
TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



YAHOO!

Archivos cifrados

NIST

**National Institute of
Standards and Technology**
U.S. Department of Commerce



dm-crypt & LUKS

https://en.wikipedia.org/wiki/Crypto_Wars

Algoritmos de cifrado

```
graph TD; A[Algoritmos de cifrado] --> B[Simétricos]; A --> C[Asimétricos]; B --> D[De bloque]; B --> E[Por hash]; D --> F[DES]; D --> G[TDEA]; D --> H[Skipjack]; D --> I[AES]; E --> J[MD5]; E --> K[SHA]; C --> L[DSA]; C --> M[EDSA]; C --> N[Diffie-Hellman]; C --> O[RSA];
```

Simétricos

De bloque

DES

TDEA

Skipjack

AES

Por hash

MD5

SHA

Asimétricos

DSA

EDSA

Diffie-Hellman

RSA

Links

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53A.pdf>

<https://www.idrix.fr/Root/content/category/7/32/46///#Download>

<https://www.keepassx.org/>

<https://securityinabox.org/en/>

https://thepiratebay.org/torrent/17357831/CIA__The_Cult_of_Secrecy

<https://www.youtube.com/watch?v=ZZ5HS8GWIec>

^video van eck phreaking

<https://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf>